International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 39-46

TRANS STELLAR
• Journal Publications • Research Consultancy

INDEMNIFYING THE CONFIDENTIALITY CONCERN OF CLOUD COMPUTING THROUGH IMPLEMENTATION OF A CIPHER CLOUD

GURPREET KAUR[1] & SUSHIL KAMBOJ[2]

[1]Student, Master of Technology, Department of Computer Science & Engineering, Shaheed Udham Singh College of Engineering & Technology, Tangori, Mohali, Punjab, India.

[2]Principal, Shaheed Udham Singh Polytechnic College, Tangori, Mohali, Punjab, India.

ABSTRACT

The cloud computing technology has brought a new era of computing with abundant benefits and ease of operations hiding all the underlying complexities thus providing an efficient platform for all categories of users. Despite of all the assets of cloud computing, its security hinders in its widespread adoption. Among the major deployments of cloud computing i.e. public cloud deployment and private cloud deployment. Private cloud is more secure as it is maintained within the organisation that is using it but at the same time setting up a private cloud infrastructure is an expensive approach. Public cloud is reasonably cost effective due to negligible infrastructure and maintenance cost but it is more vulnerable to security violations. Users need not opt for private clouds if privacy of user data is ensured in public cloud deployment.

This paper has focused on the confidentiality issues in public cloud computing environment and to overcome the same, a secure cloud architecture is proposed that enables the user to take full control and ownership of its respective data in public cloud environment. In order to achieve this, hash embedded cryptographic standards have been used, which ensures that the data remains confidential in transit as well as at rest.

KEYWORDS: Cloud Computing Security, Cipher Cloud, Confidentiality, Cryptographic Standards

INTRODUCTION

Cloud computing is TCP/IP based high development and integrations of computer technologies such as fast micro processor, huge memory, high-speed network and reliable system architecture.[1] The cloud model is composed of five essential characteristics: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service.[3] The services of cloud computing are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).[1]

There are four deployment models of cloud computing as defined by NIST:

- **Private Cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.
- **Community Cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.
- **Public Cloud:** The cloud infrastructure is provisioned for open use by the general public.

- **Hybrid Cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.[3]

Cloud computing is characterized by consumers who use cloud services as needed, who consume shared resources as a service that can rapidly and elastically scale up or down as needed, who pay only for what is used and who access services over a networked infrastructure. Cloud computing is changing the current IT delivery model for services. Benefits for business and IT include reduced costs, scalability, flexibility, capacity utilization, higher efficiencies and mobility. Predictions for growth indicate massive developments for and implementations of cloud computing services, including that the cloud computing services market is likely to reach between $150 billion in 2014 and $222.5 billion in 2015.[2]

The survey "Global survey of Consumers attitudes" in 2010 by Fujitsu Research Institute had found that 88% of people are worried about who has access to their data in the cloud and 91% of people want a system which enables them to control how their data is used. The Survey "2011 Cloud Computing outlook" in 2011 by cloud.com had found that only 61% of organizations are in the information gathering or planning states or have an approved cloud computing strategy (but no implementation), 20% have cloud implementations and 20% have no cloud computing plans. These surveys points an urgent need to find a solution which will be able to establish trust in the customers for the cloud computing strategy adoption. [5]

SECURITY ISSUES

Internet users unknowingly expose their confidential data at risk. While doing normal activities on internet, their username and passwords of emails and bank accounts along with the browsing history and other information filled in forms is stored at one place by web browser and thus it becomes vulnerable and malicious users or websites can steal the user's private information. Usually, sensitive information like user passwords is transmitted to the remote servers through non-encrypted networks. Even if encryption is used in some cases, it is only used for transmission of initial login information only while all other subsequent data is transmitted unencrypted as plain text only and hackers can easily attack this data. Hence users get exposed to potential risks when they are connected to cloud services using public networks.

Cloud Computing being the most preferred computing technology still lacks in gaining user's trust in it due to privacy concerns. Amongst the two major cloud deployment models i.e. Public Cloud Deployment Model and Private Cloud Deployment Model, the security issues are more in public cloud as compared to private cloud. Private cloud is more secure as it is maintained within the organisation that is using it but at the same time setting up a private cloud infrastructure is an expensive approach. Whereas Public cloud is reasonably cost effective due to negligible infrastructure and maintenance cost but it is more vulnerable to security violations.

Because cloud service providers are separate administrative entities, moving to the commercial public cloud deprives users of direct control over the systems that manage their data and applications. Even if cloud service provider's infrastructure and management capabilities are much more powerful and reliable than those of personal computing devices, the cloud platform still faces security threats, including media failures, software bugs, malware, administrator errors and malicious insiders.[4] If the privacy of the data stored on public cloud is ensured then it can become the most effective cloud deployment approach to be widely used. This paper discusses an approach that would enable the user to take full

control and ownership of its respective data. Not only would it make sure that the data remains segregated inside the common database framework, it would also make sure that only a particular user may access the data that it owns.

METHODOLOGY

The objective of this research work is to design a framework that ensures privacy and confidentiality of user's data on public cloud enabling the user to take full control and ownership of its respective data ensuring data segregation within the cloud. The secure cloud architecture 'Cipher Cloud' has been implemented using Platform-as-a-Service offering of Cloud Computing technology. Platform-as-a-Service is offered by various cloud service providers whereas Google's Platform-as-a-Service offering 'Google App Engine' has been used to deploy the implementation discussed in this paper.

In order to overcome the shortcomings of public cloud, we have designed and developed the Cipher Cloud framework. Out of three major CIA cloud security objectives i.e. Confidentiality, Integrity and Availability; the proposed work focuses on the 'Confidentiality' concern that covers data segregation, data lock-in and privacy. To achieve these security objectives, Cipher Cloud has been developed using the combination of an asymmetric cryptographic standard and three symmetric encryption standards. The proposed architecture has been implemented using Java runtime of Google App Engine which is a platform for developing and hosting web applications in Google-managed data centers.

The following steps are proposed to achieve the above mentioned objectives:

- Identification of suitable encryption algorithm required to support a particular criterion of key generation.
- Implementation of two-step encryption and decryption process using a combination of both asymmetric as well as symmetric data encryption algorithms on Eclipse Integrated Development Environment.
- Hosting the framework from local environment to public cloud through Google App Engine using Google Plugin for Eclipse.

Proposed Algorithm

- **Step I:** Login to Cipher Cloud using Google Account.
- **Step II:** Select an encryption standard to be used for storing the data to Blobstore.
- **Step III:** Upload the data file through the upload link at the control panel.
- **Step IV:** Encrypt the data at the client side and decrypt at the server side using RSA algorithm.
- **Step V:** Apply SHA-256 on user ID to generate the secret key and encrypt the decrypted data using symmetric encryption standard.
- **Step VI :** Store the encrypted data on the cloud.(User file is stored on the Blobstore and is mapped to the user account)
- **Step VII:** Destroy the secret key.
- **Step VIII:** Download the encrypted file from the control panel when required.

(Reversely Step V followed by Step IV to be processed for file download)

The following figure 1 shows the flowchart of the proposed work:

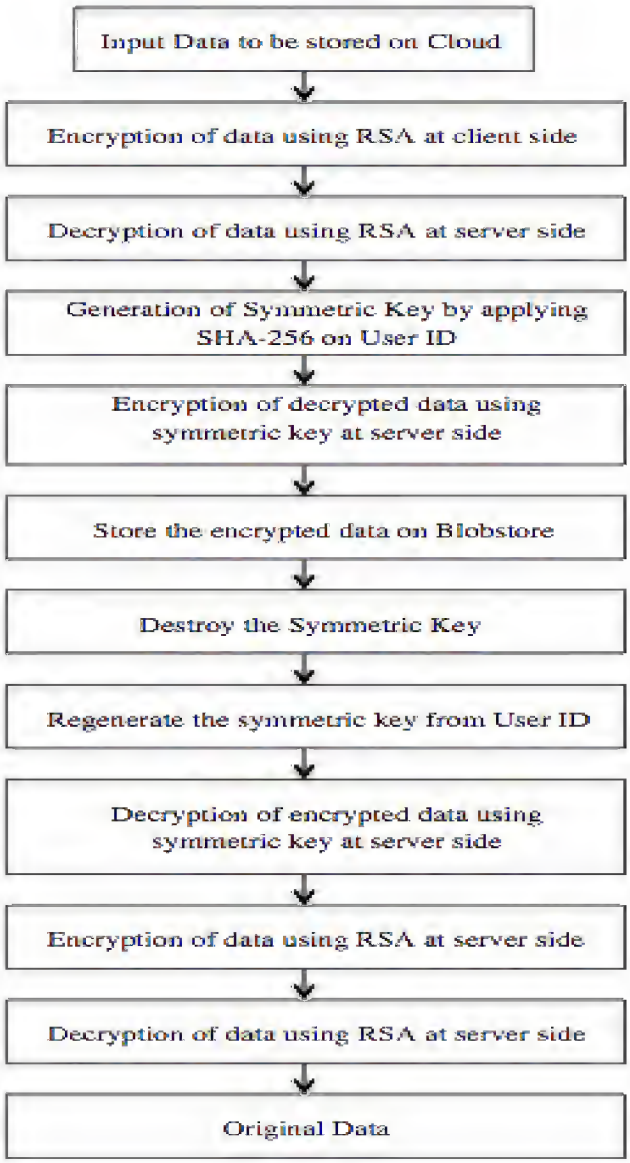

Figure 1: Flowchart of the Proposed Work

DESIGN FOCUS

The design focus of Cipher Cloud has been to bring encryption to public cloud platforms, so that users can enjoy the privacy benefits just like private clouds. With help of certain symmetric as well as asymmetric approaches of encryption, the development was accomplished. Cipher Cloud incorporates a hash embedded cryptographic process that ensures privacy of data throughout the network as well the database.

It enables the user to take full control and ownership of its respective data. Not only it makes sure that the data remains segregated inside the common database framework, it also makes sure that only a particular user may access the data that it owns. Even the database administrator cannot see the contents of the data that is being stored on the common infrastructure. In public clouds, user's data is stored in plain text format along with other user's data. Now this may create a lot of problems as the server administrator or the database administrator can have access to everyone's personal data and could even misuse it. In case of private clouds, this issue doesn't exist, as the user owns the cloud infrastructure. So keeping in mind all such privacy needs of the user, this framework has been designed.

IMPLEMENTATION

In order to fulfill the design objectives, Cipher Cloud uses a combination of asymmetric as well as symmetric encryption. The communication between client and server is secured using asymmetric techniques through a pair of public and private keys. For encrypting data for the database, symmetric algorithms have been used, as they are much faster as well as more secure compared to asymmetric techniques. This ensures that the data remains secured throughout the network and in the cloud. The user interacts with the cloud through visual interface of Cipher cloud. Asymmetric algorithm, RSA is used to encrypt the data while the data is in transit between the client and the server. Whereas symmetric algorithm is used only at the server side while saving and retrieving the data to/from the cloud.

RSA is not implemented for cloud encryption, as it is not safe to save the public or private keys in any form on the cloud. For this particular reason, the key generation mechanisms of symmetric key algorithms is used that generates the key at that very instance and destroy it as soon as it is used. Since the authentication system uses Google Accounts, each user's ID is taken to serve as the basis of user's key. Every user's ID is passed through a special hashing method, which generates a special hash value to form the basis of the key. The hash method uses the highly secured SHA-256 standard to achieve this. Hence the server has to never save the symmetric key used. It is easily generated and then destroyed, without compromising the data security, encryption or decryption process. User is permitted to opt for one of the three symmetric algorithms i.e. Advanced Encryption Standard, Triple Data Encryption Standard and Blowfish. Symmetric keys are generated as and when their request is initiated and destroyed immediately after its use. Cipher cloud never stores the encryption keys on the database, nor forces the user to remember anything else except for the authentication password. Each of these algorithms uses a specific key size, encoding, padding and initial vector.

Cipher Cloud uses Blobstore for storing user data files. Blobstore is a special database created in Google App Engine. The files stored in Blobstore are mapped to the user account and this mapping is stored in the datastore. The user is completely abstracted from what goes on in the backend of the framework. This helps make it very user friendly and at the same time ensures that the security is intact. Practical implementation of this concept required the framework implementation to be made live on a public cloud. Thus Cipher Cloud has been deployed on Google App Engine, which is a PaaS based cloud offering from Google.

RESULT ANALYSIS

The protection of highly confidential data on public cloud computing architectures could not be ensured even if most rigorous security procedures are implemented whereas such security requirements are met in private cloud computing architectures. The architecture discussed is successfully running on Google Cloud. The result analysis show that the proposed method secures the data stored on public cloud as the data stored on cloud using Cipher Cloud is not accessible to anyone except the authenticated user. The user data remains confidential in transit as well as at rest.

CONCLUSIONS AND FUTURE SCOPE

Cloud Computing technology is in a stage of consistent development and as it will proceed towards its maturity, many new and even more cloud based issues and vulnerabilities will evolve. This thesis aimed at presenting a framework that clarified the impact of cloud computing on confidentiality preservation, by making stepwise recommendations on confidentiality of data stored, processed and transmitted in cloud computing environments. Cipher cloud ensures complete privacy of user data in public cloud environment. The proposed framework achieves the objectives stated for this research

work as it removes the concern of data confidentiality in public cloud. The encryption standards ensure that data remains segregated even when data is stored on common cloud storage. Data access is permitted only after the user is authenticated thus providing full control and ownership of data to the user.

The current prevailing security questions concerning the availability and confidentiality of data in cloud computing environments are yet to be satisfactorily answered. For future research in the field of public cloud security, integrity control mechanism can be added to extend the presented framework.

REFERENCES

1. Chunye G. et al., "The characteristics of Cloud Computing", 39th International Conference on Parallel Processing Workshops, pp. 275-279, 2010.
2. Carroll, M., Merwe, A.V.D., Kotze, P., "Secure Cloud Computing", ISSA, pp. 1-9, August 2011.
3. Mell, P. and Grance T. (2011), "NIST Special Publication 800-145 : The NIST Definition of Cloud Computing", Retrieved from NIST Information Technology Laboratory, http://csrc.nist.gov/ publications/ nistpubs/ 800- 145/SP800-145.pdf
4. Ren K., Wang C. and Wang Q., "Security Challenges for the Public Cloud", Published by IEEE Computer Society, pp. 69-73, January/February 2012.
5. Gaurangkumar, K. and Minubhai, C., "To achieve Trust in the Cloud", ICACCT, pp. 16-19, 2012.
6. Astrova I., Grivas S.G and Schaaf M., "Security of a Public Cloud", ICIMISUC, pp. 564-569, 2012.
7. Google Developers, "Google App Engine", Retrieved from https://developers.google.com/appengine/docs/whatis googleappengine.
8. Jansen, W.A., "Cloud Hooks: Security and Privacy Issues in Cloud Computing", HICS 2011, pp. 1-10, January 2011.
9. Chen,D.and Zhao,H.,"Data Security and Privacy Protection Issues in Cloud Computing", ICCSEE 2012, pp. 647 – 651, March 2012.
10. Forouzan, B.A. and Fegan, S.C., "Data Communications And Networking", McGraw-HilI, Fourth Edition, 2007.
11. Gong, C., Liu, J., Zhang, Q., Chen, H. and Gong, Z., "The Characteristics of Cloud Computing", 39th International Conference on Parallel Processing Workshops, pp. 275-279, 2010.
12. Ming, T. and Yongsheng, Z., "Analysis of Cloud Computing and Its Security", International Symposium on Information Technology In Medicine And Education, Volume-1, pp. 379-381, 2012.
13. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication 800-22 Revision 1a, April 2010.
14. Wang. X., Wang. B. and Huang, J., "Cloud computing and its key techniques", International Conference on Computer Science and Automation Engineering, Volume-2, pp. 404 – 410, 2011.

15. Zhou M., Zhang R. , Xie W., Qian W. and Zhou A. , "Security and Privacy in Cloud Computing: A Survey", ICSKG, pp. 105 – 112, November 2010.
16. Wu, J., Ping, L., Ge, X., Wang, Y. and Fu, J., "Cloud Storage as the Infrastructure of Cloud Computing", International Conference on Intelligent Computing and Cognitive Informatics, pp.380-383, 2010.
17. Kaufman, L.M., "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Volume-7, Issue-4, pp. 61 – 64, July-August 2009.
18. Kantarcioglu, M. , Bensoussan, A. and SingRu Hoe, "Impact of security risks on cloud computing adoption", AACCCC, pp. 670 – 674, September 2011.
19. Yang, J., Chen, Z. , "Cloud Computing Research and Security Issues", International Conference on Computation al Intelligence and Software Engineering, pp.1-3, December 2010.
20. Hoff, C., Simmonds, P., Pohlman, M., Swain, B., Posey, L. et al., "Security Guidance for Critical Area of Focus in Cloud Computing V3. 0", Retrieved from Cloud Security Alliance, fromhttps://downloads.cloud securityalliance.org/initiatives/guidance/csaguide.v3.0.pdf, November 2011.
21. Iankoulova, I. and Daneva, M., "Cloud Computing Security Requirements: a Systematic Review", Sixth International Conference on Research Challenges in Information Science, pp.1-7, 2012.
22. Tianfield, H., "Cloud Computing Architectures", IEEE International Conference on Systems, Man and Cybernetics (SMC), pp. 1394 – 1399, 2011.